105 - Groupe des permutations d'un ensemble fini. Applications

Alexis Guérin

Un des premiers mathématiciens à vouloir formaliser le groupe des permutations est Evariste Galois. Le travail de Galois proprement dit est fondé sur l'étude des « substitutions » des racines des polynômes appelées aujourd'hui permutations. C'est lors de l'étude de ces substitutions de racines qu'il est amené à théoriser la notion de groupe pour mieux décrire les propriétés de celles-ci. Depuis, la théorie des groupes s'est largement développée et a montré que le groupe des permutations était en fait un des groupes fondamentaux de sa théorie grâce au théorème de Cayley.

Table des matières

1 Les généralités du groupe symétrique.

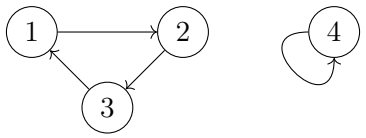
1.1 Les généralités.

Définition 1.1 Soit E un ensemble non vide. L'ensemble des bijections de E sur lui même est un groupe pour la composition des applications, appelé *groupe des permutations de E* ou *groupe symétrique de E*, et est noté $\mathfrak{S}_E$. Un élément de $\mathfrak{S}_E$ est appelé *permutation.*

Pour $E = [\![1, n]\!]$ on notera le groupe des permutations de cet ensemble $\mathfrak{S}_n := \mathfrak{S}_E$. Pour $\sigma \in \mathfrak{S}_n$ on utilisera la notation suivante :

$$\begin{pmatrix} 1 & \cdots & \text{n} \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

Exemple 1.2 Pour $E = [\![1, 4]\!]$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, on peut illustrer la permutation correspondante grâce au schéma suivant :



Propriété 1.3 Soient E, E' deux ensembles non vides, si E et E' sont en bijection, alors il existe un isomorphisme de groupe de $\mathfrak{S}_E$ vers $\mathfrak{S}_{E'}$.

Preuve : Soit $f : E \to E'$ une bijection. Elle induit alors l'application $\tilde{f}$ suivante

$$\tilde{f} : \left| \begin{array}{ccc} \mathfrak{S}_E & \longrightarrow & \mathfrak{S}_{E'} \\ \sigma & \longmapsto & f \circ \sigma \circ f^{-1} \end{array} \right.$$

dont il est facile de vérifier que c'est isomorphisme de groupe entre $\mathfrak{S}_E$ et $\mathfrak{S}_{E'}$.

□

Remarque 1.4 Soit E un ensemble fini de cardinal n, alors E est en bijection avec l'ensemble $[\![1, n]\!]$. Ainsi, en utilisant la propriété précédente, $\mathfrak{S}_E$ est isomorphe à $\mathfrak{S}_n$. Grâce à cette remarque nous pouvons restreindre l'étude des groupes symétriques à celles des groupes de la forme $\mathfrak{S}_n$.

Propriété 1.5 Le cardinal de $\mathfrak{S}_n$ est $n!$.

Définition 1.6 On définit *le support* d'un permutation $\sigma \in \mathfrak{S}_n$ comme étant l'ensemble suivant :

$$Supp(\sigma) := \{i \in [\![1, n]\!] \mid \sigma(i) \neq i\}.$$

Autrement dit $Supp(\sigma) = [\![1, n]\!] \setminus Fix(\sigma)$ où $Fix(\sigma)$ est l'ensemble des points fixes de σ.

Exemple 1.7 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ a comme support $Supp(\sigma) = \{1, 2, 3\}$.

Propriété 1.8 Soient $\sigma, \sigma' \in \mathfrak{S}_n$ avec $n > 2$ alors :

1. $\sigma(Supp(\sigma)) = Supp(\sigma)$
2. $Supp(\sigma) = Supp(\sigma^{-1})$

3. $Supp(\sigma \circ \sigma') \subset Supp(\sigma) \cup Supp(\sigma')$ et on égalité lorsque $Supp(\sigma) \cap Supp(\sigma') = \varnothing$ (σ et σ' sont alors dites à support disjoint)

Exemple 1.9 Nous donnons ici un exemple où deux permutations ne sont pas à support disjoint et où le support de la composition de ces deux permutations n'est clairement pas égal à l'union des supports des deux permutations concernées :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad \text{et} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

En effet $\sigma' = \sigma^{-1}$, donc $Supp(\sigma \circ \sigma') = \varnothing$ alors que $Supp(\sigma) = Supp(\sigma') = [\![1, 4]\!]$.

Propriété 1.10 Deux permutations à support disjoint commutent.

Preuve : Soient σ et σ' deux permutations à support disjoint alors,

$$[\![1, n]\!] = \big(Fix(\sigma) \cap Fix(\sigma')\big) \cup Supp(\sigma) \cup Supp(\sigma').$$

Si $i \in Fix(\sigma) \cap Fix(\sigma')$ on a alors, $\sigma(\sigma'(i)) = \sigma(i) = i = \sigma'(i) = \sigma'(\sigma(i))$.
Si $i \in Supp(\sigma)$, alors par hypothèse $i \in Fix(\sigma')$. De plus par la propriété 1.8, $\sigma(i) \in Supp(\sigma) \subset Fix(\sigma')$ par hypothèse. Donc $\sigma(\sigma'(i)) = \sigma(i) = \sigma'(\sigma(i))$.
On conclut en raisonnant de la même façon pour $i \in Supp(\sigma')$.

□

1.2 La décomposition en produit de cycles.

Soit $\sigma \in \mathfrak{S}_n$. On peut restreindre l'action naturelle de $\mathfrak{S}_n$ sur $\{1, ..., n\}$ à celle du sous groupe $< \sigma >$ sur $\{1, ..., n\}$. Il est alors facile de décrire les orbites, appelés σ-orbites, de cette action :

$$Orb_\sigma(i) = \{\sigma^m(i) \mid m \in \mathbb{Z}\}.$$

Ces orbites forment une partition de $[\![1, n]\!]$, elles sont donc de cardinal fini. En particulier, il existe u et v des entiers relatifs (avec $u < v$) tel que $\sigma^u(i) = \sigma^v(i)$ donc $\sigma^{v-u}(i) = i$ avec $v - u \in \mathbb{N}^*$. En notant p le plus petit entier naturel strictement positif tel que $\sigma^p(i) = i$ on peut affiner la description des σ-orbites. En effet pour tout m entier relatif, en réalisant la division euclidienne de m par p : $m = kp + r$ avec $k \in \mathbb{Z}$ et $r \in [\![0, p-1]\!]$, on a $\sigma^m(i) = \sigma^{kp+r}(i) = \sigma^r(\sigma^{kp}(i)) = \sigma^r(i)$. Donc

$$Orb_\sigma(i) = \{\sigma^m(i) \mid m \in [\![0, p-1]\!]\}.$$

On peut alors remarquer que l'union des σ-orbites non réduites à un singleton est le support de σ. La description des σ-orbites nous amène à la définition suivante :

Définition 1.11 On dit qu'une permutation $\sigma \in \mathfrak{S}_n$ est un *cycle* s'il n'existe qu'une σ-orbite qui n'est pas réduite à un singleton.
Si $p \geq 2$ est le nombre d'éléments de $Supp(\sigma)$, on dit alors que σ est un *p-cycle*. Un 2-cycle est aussi appelé transposition.
Soit σ un p-cycle tel que sa seule σ-orbite non réduite à un singleton soit de la forme :
$\{a_1, a_2 := \sigma(a_1), ..., a_p := \sigma^{p-1}(a_1)\}$. On le notera alors $(a_1 a_2 ... a_p)$.

Exemple 1.12 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ est un 3-cycle car $Orb_\sigma(1) = \{1, 2, 3\}$ et $Orb_\sigma(4) = \{4\}$.
Avec la notation introduite dans la définition 1.11 $\sigma = (1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$.

On va maintenant montrer que chaque permutation se décompose en produit de cycles à supports disjoints.

Lemme 1.13 Soit $\sigma \in \mathfrak{S}_n$, et soit ω une orbite non réduite à un élément. On note σ_ω la permutation suivante :

$$\sigma_\omega(a) = \sigma(a) \text{ si } a \in \omega \text{ et } \sigma_\omega(a) = a \text{ si } a \notin \omega.$$

Alors σ_ω est un cycle de support ω, et pour tout $a \in \omega$, on a

$$\sigma_\omega = (a\ \sigma(a)\ \dots\ \sigma^{p-1}(a)).$$

où p est le nombre d'éléments de ω.
De plus tous les p-cycles de $\mathfrak{S}_n$ sont de cette forme.

Théorème 1.14 Soit $\sigma \in \mathfrak{S}_n$. Alors σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près. Cette décomposition est donnée par :

$$\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega.$$

où Ω^* est l'ensemble des σ-orbites non réduites à un singleton.

Preuve : Montrons d'abord l'égalité $\sigma = \prod_{\omega\in\Omega^*} \sigma_\omega$.
Soit a un point fixe de σ, alors $a \notin \omega$ pour $\omega \in \Omega^*$. En effet s'il existe $\omega \in \Omega^*$ tel que $a \in \omega$ alors ω est un singleton ce qui, d'après la définition de Ω^*, est absurde. Donc $\forall w \in \Omega^*\ \sigma_\omega(a) = a$. Ce qui nous permet d'affirmer que $\prod_{\omega\in\Omega^*} \sigma_\omega(a) = a = \sigma(a)$.
Si a est dans le support de σ alors il existe $\omega_0 \in \Omega^*$ tel que $a \in \omega_0$ et $\forall \omega \in \Omega^* \setminus \{\omega_0\}\ a \notin \omega$ car les éléments de Ω^* sont disjoints. Par conséquent, $\sigma_{\omega_0}(a) = \sigma(a)$ et $\sigma_\omega(a) = a$ pour tout $\omega \neq \omega_0$ et donc comme les support des cycles σ_ω sont disjoints, ces permutations commutent et on a :

$$\prod_{\omega\in\Omega^*} \sigma_\omega(a) = \sigma_{\omega_0}\left(\left(\prod_{\omega\in\Omega^*\setminus\omega_0} \sigma_\omega\right)(a)\right) = \sigma_{\omega_0}(a) = \sigma(a).$$

On a donc prouvé que $\prod_{\omega\in\Omega^*} \sigma_\omega = \sigma$.

Montrons maintenant l'unicité de cette décomposition.
Soit $\sigma = \sigma_1 \cdots \sigma_r$ une autre décomposition de σ tel que les σ_i sont à supports disjoints. On note E_i le support du cycle σ_i. On va montrer que E_i est une σ-orbite non réduite à un élément. Soit $a \in E_i$, comme les supports des σ_i sont disjoints, on a $\sigma_j(a) = a$ dès que $j \neq i$. De plus, puisque les σ_j commutent, on a :

$$\sigma(a) = \left(\prod_j \sigma_j\right)(a) = \sigma_i\left(\left(\prod_{j\neq i} \sigma_j\right)(a)\right) = \sigma_i(a).$$

On a donc $\sigma_i(a) = \sigma(a)$ si $a \in E_i$. Puisque $E_i = Supp(\sigma_i)$ est stable par σ_i, on a donc $\sigma(a) = \sigma_i(a) \in E_i$. Par récurrence on obtient que $\sigma_i^k(a) = \sigma^k(a)$ pour $k \geqslant 0$.
Comme σ_i est un cycle de support E_i, alors E_i forme une σ_i-orbite non réduite à un élément. Le lemme 1.13 appliqué à σ_i montre alors que le support est $E_i = \{a, \sigma_i(a), \dots, \sigma_i^{p_i-1}(a)\}$ où p_i est le cardinal de E_i. Par ce qui précède, on obtient donc

$$E_i = \{a, \sigma(a), \dots, \sigma^{p_i-1}(a)\}.$$

Ainsi, les éléments de E_i forment une σ-orbite (à savoir celle de a) non réduite à un élément.
Remarquons alors que, puisque le support de σ est la réunion des E_i, on obtient bien toutes les orbites non réduites à un élément. Cela prouve l'unicité de la décomposition, et achève la démonstration.

□

Remarque 1.15 On a donc établi que toutes permutations σ de $\mathfrak{S}_n$ peut s'écrire de la façon suivante :

$$\sigma = (a_1\ \sigma(a_1)\ \ldots\ \sigma^{p_1-1}(a))\ldots(a_r\ \sigma(a_r)\ \ldots\ \sigma^{p_r}(a_r)).$$

Pour trouver cette décomposition pour une permutation σ de $\mathfrak{S}_n$, on cherche d'abord le cycle qui contient k, où k est le premier élément de $[\![1, n]\!]$ qui n'est pas un point fixe (qui existe si σ n'est pas l'identité, ce que l'on suppose puisque la décomposition de l'identité en cycle à support disjoint est direct). Pour cela on regarde les $\sigma^i(k)$ jusqu'au premier i_0 tel que $\sigma^{i_0}(k) = k$. Alors le cycle recherché est

$$(1\ \sigma(1)\ \ldots\ \sigma^{k_0-1}(1)).$$

On recommence ce processus pour chaque élément de $[\![1, n]\!]$ qui n'est pas un point fixe et qui n'appartient pas à un des cycles déjà exhibés.

Exemple 1.16 On considère la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 5 & 1 & 6 & 8 & 2 \end{pmatrix} \in \mathfrak{S}_8$.
L'élément 1 n'est pas un point fixe de σ et :

$$\sigma(1) = 4\ \ \sigma(4) = 5\ \ \sigma(5) = 1.$$

Donc le premier cycle que l'on obtient est (1 4 5). On choisit maintenant un entier distinct de $1, 4$ et 5 qui n'est pas un point fixe de σ, disons 2. On obtient alors le cycle : (2 3 7 8). Qui était le dernier cycle à trouver puisque 6 est une point fixe de σ. Donc

$$\sigma = (1\ 4\ 5)(2\ 3\ 7\ 8).$$

Propriété 1.17 Un p-cycle est d'ordre p.

Preuve : Soit $\sigma = (a_1\ \ldots\ a_p)$. Pour $j \in [\![1, p-1]\!]$, on a

$$\sigma^j(a_1) = a_{k+1} \neq a_1.$$

Donc $\sigma, \sigma^2, \ldots, \sigma^{p-1}$ ne sont pas égaux à Id. En revanche pour $k \in [\![1, n]\!]$, on a

$$\sigma^p(a_k) = \sigma^p(\sigma^{k-1}(a_1)) = \sigma^{k-1}(\sigma^p(a_1)) = \sigma^{k-1}(a_1) = a_k.$$

Donc $\sigma^p = Id$. Donc $o(\sigma) = p$.

□

Propriété 1.18 Soient $\sigma_1, \sigma_2, \ldots, \sigma_r \in \mathfrak{S}_n$ des permutations à supports deux à deux disjoints. Alors, on a

$$o(\sigma_1 \ldots \sigma_r) = ppcm(o(\sigma_1), \ldots, o(\sigma_r)).$$

On déduit donc des deux propriétés précédentes le théorème suivant :

Théorème 1.19 L'ordre d'une permutation est le ppcm des longueurs des cycles à supports disjoints qui la composent.

Exemple 1.20 Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 7 & 5 & 1 & 9 & 8 & 2 & 6 \end{pmatrix}$.
La décomposition en cycles à supports disjoints de σ est $\sigma = (1\ 4\ 5)(2\ 3\ 7\ 8)(6\ 9)$. En utilisant le théorème précédent :

$$o(\sigma) = ppcm(3, 4, 2) = 12.$$

Une autre utilisation du théorème de décomposition des permutations en cycles à supports disjoints est la description des classes de conjugaisons de $\mathfrak{S}_n$.

Propriété 1.21 Soit $\tau \in \mathfrak{S}_n$. Pour tout p-cycle $(a_1\ \dots\ a_p)$, on a

$$\tau(a_1\ \dots\ a_p)\tau^{-1} = (\tau(a_1)\ \dots\ \tau(a_p)).$$

En particulier, le conjugué d'un cycle est un cycle de même longueur.

Preuve : Soit $\tau' = \tau(a_1\ \dots\ a_p)\tau^{-1}$. Alors, on a

$$\tau'(\tau(a_i)) = \tau((a_1\ \dots\ a_p)(a_i)) = \tau(a_{i+1}) \text{ si } i \in [\![1, p-1]\!]$$

et

$$\tau'(\tau(a_p)) = \tau((a_1\ \dots\ a_p)(a_p)) = \tau(a_1).$$

Soit maintenant $a \in [\![1, n]\!] \setminus \{\tau(a_1), \dots, \tau(a_p)\}$. Puisque τ est bijective, donc injective, on en déduit que $\tau^{-1}(a) \neq a_i$, pour tout $i \in [\![1, p]\!]$. En particulier, le p-cycle $(a_1\ \dots\ a_p)$ fixe $\tau^{-1}(a)$, et l'on a donc

$$\tau'(a) = \tau(\tau^{-1}(a)) = a.$$

Ce qui achève la démonstration.

□

Théorème 1.22 Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si, et seulement si, les listes (avec répétition) des longueurs des cycles à supports disjoints qui les composent sont les mêmes à l'ordre près.

Preuve : Soit $\sigma = \sigma_1\sigma_2 \dots \sigma_r$, où les σ_i sont des cycles à supports disjoints. Soit $\sigma' \in \mathfrak{S}_n$. Supposons que σ et σ' sont conjuguées, alors il existe $\tau \in \mathfrak{S}_n$ tel que $\tau\sigma\tau^{-1} = \sigma'$. De plus,

$$\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1} \dots \tau\sigma_r\tau^{-1}.$$

D'après la propriété précédente $\sigma'_i := \tau\sigma_i\tau^{-1}$ est un cycle de même longueur que σ_i. De plus le support de σ'_i est l'image de σ_i par τ donc, les supports des σ_i étant disjoints, comme τ est bijective les supports des σ'_i sont eux aussi disjoints. Ainsi $\sigma' = \sigma'_i \dots \sigma'_r$ est la décomposition en cycle à support disjoint de σ'. Donc les listes des longueurs des cycles à supports disjoints qui composent σ et σ' sont les mêmes.
Réciproquement, soient $\sigma, \sigma' \in \mathfrak{S}_n$. Considérons alors leurs décompositions en cycles à supports disjoints :

$$\sigma = \sigma_1 \dots \sigma_r \quad \sigma' = \sigma'_1 \dots \sigma'_r.$$

On suppose que σ_i est de même longueur que σ'_i, quitte à ré-indexer les cycles de σ'_i. On note :

$$\sigma_i = (a_1^{(i)} \dots a_{p_i}^{(i)}) \quad \sigma_i = (b_1^{(i)} \dots b_{p_i}^{(i)}).$$

On sait avec la propriété 1.8 que

$$Supp(\sigma) = \bigcup_{i=1}^{r} Supp(\sigma_i) = \bigcup_{i=1}^{r} Supp(\sigma'_i) = Supp(\sigma')$$

et donc, on a aussi :

$$[\![1, n]\!] \setminus Supp(\sigma) = [\![1, n]\!] \setminus Supp(\sigma').$$

On note alors f une bijection quelconque entre $[\![1, n]\!] \setminus Supp(\sigma)$ et$[\![1, n]\!] \setminus Supp(\sigma')$ et on introduit $\tau : [\![1, n]\!] \to [\![1, n]\!]$ défini par :

$$\tau(a_j^{(i)}) = b_j^{(i)} \quad \text{et} \quad \tau(a) = f(a) \text{ si } a \neq a_j^{(i)}.$$

L'élément τ défini bien une permutation de $[\![1, n]\!]$ dans $[\![1, n]\!]$ et elle vérifie $\tau\sigma_i\tau^{-1} = \sigma'_i$ pour $i \in [\![1, r]\!]$. Donc τ vérifie aussi la relation $\tau\sigma\tau^{-1} = \sigma'$. Ainsi σ et σ' sont conjugués.

□

1.3 Les générateurs de $\mathfrak{S}_n$

Dans la section 1.2 le théorème 1.14 nous a permis d'exhiber un premier ensemble de générateurs de $\mathfrak{S}_n$, les cycles. Grâce à ce résultat nous allons trouver d'autres systèmes de générateurs de $\mathfrak{S}_n$.

Propriété 1.23 Tous les cycles de longueur p de $\mathfrak{S}_n$ peuvent s'écrire comme produit de $p - 1$ transpositions.

Preuve : Soit $(a_1\ a_2\ \dots\ a_p)$ un p-cycle de $\mathfrak{S}_n$ alors

$$(a_1\ a_2\ \dots\ a_p) = (a_1\ a_2)(a_2\ a_3)\dots(a_{p-2}\ a_{p-1})(a_{p-1}\ a_p).$$

□

Corollaire 1.24 $\mathfrak{S}_n$ est engendré par les transpositions.

Propriété 1.25 La parité du nombre de transpositions nécessaires pour décomposer une permutation ne dépend pas de la décomposition choisie.

Propriété 1.26 Toutes les transpositions de $\mathfrak{S}_n$ peut s'écrire comme produit de 3 transpositions de la forme $(1\ i)$ avec $i \in [\![2, n]\!]$.

Preuve : Soit une transposition $(i\ j)$ de $\mathfrak{S}_n$, alors $(i\ j) = (1\ i)(1\ j)(1\ i)$

□

Corollaire 1.27 Les transpositions de la forme $(1\ i)$ avec $i \in [\![2, n]\!]$ engendrent $\mathfrak{S}_n$.

Propriété 1.28 Toutes les transpositions de $\mathfrak{S}_n$ peut s'écrire comme produit de transpositions de la forme $(i\ i+1)$ avec $i \in [\![1, n-1]\!]$.

Preuve : Soit $(i\ j)$ une transposition de $\mathfrak{S}_n$ alors avec la propriété 1.21 on a

$$(i\ i+1\cdots j-1)(j-1\ j)(i\ i+1\cdots j-1)^{-1} = (i\ j).$$

Or la propriété 1.23 nous assure que $(i\ i+1\cdots j-1) = (i\ i+1)\dots(j-2\ j-1)$ et comme $(i\ i+1)^{-1} = (i\ i+1)$, on obtient le résultat.

□

Corollaire 1.29 Le transpositions de la forme $(i\ i+1)$ avec $i \in [\![1, n-1]\!]$ engendrent $\mathfrak{S}_n$.

Propriété 1.30 Le groupe $\mathfrak{S}_n$ est engendré par $(1\ 2)$ et $(1\ 2 \dots n)$.

Preuve : Pour $i \in [\![1, n-1]\!]$, on a

$$(i\ i+1) = (1\ 2 \dots n)^{i-1}(1\ 2)(1\ 2 \dots n)^{1-i}.$$

□

2 Des propriétés autour du groupe symétrique.

2.1 La signature d'une permutation et le groupe alterné

Définition 2.1 Soit $n \geqslant 1$ et soit $\sigma \in \mathfrak{S}_n$. Si σ se décompose en produit de r transpositions, *la signature* de σ est l'élément :

$$\varepsilon(\sigma) = (-1)^s.$$

Remarque 2.2 C'est la propriété 1.25 qui nous assure de la bonne définition de la signature.

Propriété 2.3 Soit $n \geqslant 2$, la signature vérifie les propriétés suivantes :

1. $\varepsilon(Id) = 1$
2. Toute transposition est de signature -1
3. pour toutes permutations σ, $\sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$
4. Pour tout $\sigma \in \mathfrak{S}_n$, on a $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)^{-1}$

Preuve : 3. Soient σ et σ' deux permutations qui s'écrivent respectivement comme produit de s et t transpositions. Alors $\sigma\sigma'$ s'écrit comme produit de $s+t$ transpositions. Donc

$$\varepsilon(\sigma\sigma') = (-1)^{s+t} = (-1)^s(-1)^t = \varepsilon(\sigma)\varepsilon(\sigma')$$

□

Théorème 2.4 On suppose que $n \geqslant 2$. Alors il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \to \mathbb{C}^\times$ non trivial. Si $\sigma \in \mathfrak{S}_n$ s'écrit comme produit de s transpositions, alors on a

$$\varepsilon(\sigma) = (-1)^s.$$

Preuve : L'existence d'un tel morphisme est assuré par le point 3 de la propriété 2.3.
Discutons de l'unicité d'un tel morphisme. Soit $\varepsilon' : \mathfrak{S}_n \to \mathbb{C}^\times$ un morphisme de groupes non trivial. Remarquons dans un premier temps que ε' est constant sur les classes de conjugaison de $\mathfrak{S}_n$. En effet, si $\sigma' = \tau\sigma\tau^{-1}$, on a

$$\varepsilon'(\sigma') = \varepsilon'(\tau\sigma\tau^{-1}) = \varepsilon'(\tau)\varepsilon'(\sigma)\varepsilon'(\tau)^{-1} = \varepsilon'(\sigma).$$

En particulier, toutes les transpositions de $\mathfrak{S}_n$ ont même image par ε'. De plus comme pour toutes transpositions τ de $\mathfrak{S}_n$ on a la relation $\tau^2 = Id$, on a $\varepsilon'(\tau)^2 = 1$ donc $\varepsilon'(\tau) = 1$ ou -1. Or si $\varepsilon'(\tau) = 1$ alors en utilisant le corollaire 1.24 on peut affirmer que ε' est en fait l'identité, ce qui n'est pas possible. Donc $\varepsilon'(\tau) = -1$ pour toutes transpositions τ, et donc $\varepsilon'(\sigma) = (-1)^s$si σ est produit de s transpositions.
Ce qui achève la preuve de l'unicité et donc la preuve.

□

Exemple 2.5 En utilisant la propriété 1.23 on peut affirmer que la signature d'un p-cycle est égale à $(-1)^{p-1}$.

Propriété 2.6 (Quelques expressions alternatives de la signature)
Soit $\sigma \in \mathfrak{S}_n$ alors,

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

mais encore,

$$\varepsilon(\sigma) = (-1)^{n - N_\sigma}.$$

où N_σ est le nombre de σ-orbites.

Définition 2.7 Le *groupe alterné* de $\mathfrak{S}_n$ est le noyau de la signature. On le notera $\mathfrak{A}_n$. En d'autres termes,

$$\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \text{ tel que } \varepsilon(\sigma) = 1\}.$$

Propriété 2.8 Le groupe $\mathfrak{A}_n$ vérifie les propriétés suivantes :

1. $\mathfrak{A}_n$ est un sous groupe distingué et d'indice 2 de $\mathfrak{S}_n$
2. $\#\mathfrak{A}_n = \frac{n!}{2}$
3. Si $n = 2$, $\mathfrak{A}_n$ est trivial, si $n = 3$ $\mathfrak{A}_n$ est cyclique, engendré par un 3-cycle.

Propriété 2.9 Si $n \geqslant 3$, le groupe alterné est engendré par chacune des familles suivantes :

1. les produits de deux transpositions
2. les 3-cycles

Preuve :

1. Cette propriété découle directement du corollaire 1.24 et de la définition de $\mathfrak{A}_n$.
2. Pour montrer le deuxième point nous allons utiliser le premier point, en montrant que tous produits de deux transpositions s'écrit comme produit de 3-cycles. Soient τ_1, τ_2 deux transpositions, alors si τ_1 et τ_2 ont le même support $\tau_1\tau_2 = Id$. Si le support de τ_1 et le support de τ_2 partagent un élément alors $\tau_1 = (a\ b)$, $\tau_2 = (b\ c)$ et donc $\tau_1\tau_2 = (a\ b\ c)$. Enfin si les supports de τ_1 et de τ_2 sont disjoints, ie $\tau_1 = (a\ b)$ et $\tau_2 = (c\ d)$ avec $a, b, c, d \in [\![1, n]\!]$ distincts, alors $\tau_1\tau_2 = (a\ c\ b)(a\ c\ d)$.

□

Nous allons maintenant démontrer que $\mathfrak{A}_n$ est simple pour $n \geqslant 5$. Ce résultat dû à Galois, est central dans la preuve de l'impossibilité de résoudre par radicaux une équation polynomiale générale de degré $n \geqslant 5$.

Propriété 2.10 Si $n \geqslant 5$ alors les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Théorème 2.11 On suppose que $n \geqslant 3$. Alors, le groupe alterné $\mathfrak{A}_n$ est simple si et seulement si, $n \neq 4$.

Preuve :

Le cas $n = 3$ se traite rapidement à partir du moment où l'on sait que $\mathfrak{A}_3$ est engendré par un 3-cycle.

Pour le cas $n = 4$, le groupe de Klein défini ainsi :

$$V_4 = \{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

est un sous groupe non trivial et distingué de $\mathfrak{A}_4$.

Passons maintenant eu cas $n \geqslant 5$. Soit H un sous groupe distingué de $\mathfrak{A}_n$. Avant de s'attaquer au problème, faisons trois remarques préliminaires.

1. Si H contient un 3-cycle, alors $H = \mathfrak{A}_n$. En effet comme H est distingué dans $\mathfrak{A}_n$ et que d'après la propriété 2.10, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$, si H en contient l'élément 1, alors il les contient tous. De plus la propriété 2.9 nous assure que les 3-cycles engendrent $\mathfrak{A}_n$. Donc $H = \mathfrak{A}_n$.
2. Si $\sigma \in H$ et $\tau \in \mathfrak{A}_n$ alors $\sigma\tau\sigma^{-1}\tau^{-1} \in H$. En effet comme H est distingué alors $\tau\sigma\tau^{-1} \in H$. On conclut en utilisant le fait que H est un groupe.
3. Si H contient un produit de deux transpositions à support disjoint alors H contient un 3-cycle et en particulier $H = \mathfrak{A}_n$. En effet, si on suppose que $\sigma = (a\ b)(c\ d) \in H$ avec $a, b, c, d \in [\![1, n]\!]$ tous différents. Or, comme $n \geqslant 5$ alors il existe $e \notin \{a, b, c, d\}$. On pose $\tau = (a\ b\ e)$, on a alors

$$\tau\sigma^{-1}\tau^{-1} = \tau(c\ d)\tau^{-1}\tau(a\ b)\tau^{-1} = (c\ d)(b\ e)$$

Donc $\sigma\tau\sigma^{-1}\tau^{-1} = (a\ b)(c\ d)(c\ d)(b\ e) = (a\ b\ e) \in H$ avec le point 2 et on obtient que $H = \mathfrak{A}_n$.

Avec les trois remarques précédentes, si on suppose que H n'est pas trivial, il nous suffit de montrer qu'un 3-cycle ou le produit de deux transpositions à supports disjoints appartient à H pour conclure. On suppose donc que H n'est pas trivial : soit $\sigma \in H \setminus \{Id\}$.

On suppose dans un premier temps qu'il n'y a que des 3-cycles dans la décomposition en cycles à supports disjoints de σ. S'il n'y en a qu'un c'est terminé. Sinon, il y en a au moins deux : $(a\ b\ c)$ et $(d\ e\ f)$. On considère alors $\tau = (a\ d)(b\ e)$. Alors avec le point 2, la permutation $\sigma' = \sigma\tau\sigma^{-1}\tau^{-1} \in H$. Or,

$$\sigma\tau\sigma^{-1} = (\sigma(a)\ \sigma(d))(\sigma(b)\ \sigma(e)) = (b\ e)(c\ f).$$

Donc,

$$\sigma\tau\sigma^{-1}\tau^{-1} = (b\ e)(c\ f)(b\ e)(a\ d) = (c\ f)(a\ d) \in H.$$

On suppose que la décomposition en cycles à supports disjoints ne contienne pas que des 3-cycles. On admet provisoirement qu'il existe une partie $F \subset [\![1, n]\!]$ tel que F soit de cardinal 3 et $F \cup \sigma(F)$ contienne exactement 4 éléments. On pose alors τ un cycle de support F. C'est donc un 3-cycle, et donc $\tau \in \mathfrak{A}_n$. On a de plus

$$Supp(\sigma\tau\sigma^{-1}) = \sigma(F) \neq F = Supp(\tau).$$

En particulier $\sigma\tau\sigma^{-1} \neq \tau$ et donc $\sigma' := \sigma\tau\sigma^{-1}\tau^{-1} \neq Id$. De plus le point 2 nous assure que $\sigma' \in H$. La propriété 1.8 nous assure que :

$$Supp(\sigma') \subset Supp(\sigma\tau\sigma^{-1}) \cup Supp(\tau^{-1}) = \sigma(F) \cup F.$$

Comme $\sigma(F) \cup F$ est de cardinal 4 et que $\sigma' \neq Id$ alors σ' est soit un 3-cycle soit un produit de deux transpositions à supports disjoints. En effet les 4-cycles et les transpositions ne sont pas des éléments de $\mathfrak{A}_n$. Donc $H = \mathfrak{A}_n$.

Prouvons l'existence de F. S'il existe un cycle de longueur $\geqslant 4$ dans la décomposition de σ en cycles à supports disjoints, $(a\ b\ c\ d \ldots)$ par exemple, alors il nous suffit de prendre $F = \{a, b, c\}$ car

$$F \cup \sigma(F) = \{a, b, c, d\}.$$

Sinon, par hypothèse, σ admet au moins une transposition dans sa décomposition en cycles à supports disjoints, alors σ en admet en fait, au moins deux. Dans le cas contraire σ s'écrirait comme produit de 3-cycle et d'une transposition. Donc $\varepsilon(\sigma) = -1$, ce qui est absurde car $\sigma \in H \subset \mathfrak{A}_n$. On note $(a\ b)$ et $(c\ d)$ ces deux transpositions. Alors $F = \{a, b, c\}$ convient. Ce qui achève la preuve.

□

Corollaire 2.12 On suppose $n \geqslant 3$, on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \neq 4$. De plus pour $n \geqslant 3$ $D(\mathfrak{A}_n) = \mathfrak{A}_n$.

Propriété 2.13 Pour $n \geqslant 3$ le centre de $\mathfrak{S}_n$ est trivial.

Corollaire 2.14 Pour $n \geqslant 2$, si $n \neq 4$, les sous groupes distingués de $\mathfrak{S}_n$ sont

$$\{Id\} \quad \mathfrak{A}_n \quad \text{et} \quad \mathfrak{S}_n$$

2.2 Les automorphismes de $\mathfrak{S}_n$

La description des automorphismes d'un groupe s'avère être utile dans les calculs des extentions de ce même groupe et plus particulièrement dans la confection des lois de ces extentions qui font intervenir la notion de produit semi-direct.

Définition 2.15 Soit G un groupe et φ un endomorphisme de G. On dit que φ est un automorphisme intérieur de G s'il existe $g \in G$ tel que pour tout $h \in G$ $\varphi(h) = ghg^{-1}$. On note $Int(G)$ l'ensemble des automorphismes intérieurs de G.

Lemme 2.16 Soit G un groupe et φ un automorphisme de G. Alors l'image d'une classe de conjugaison par φ est une classe de conjugaison.

Dans la suite nous supposerons que $n \geqslant 3$.

Théorème 2.17 Pour $n \neq 6$, tous les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs. En d'autres termes on a :

$$Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$$

Avant d'aborder la démonstration du théorème nous allons prouver le lemme suivant :

Lemme 2.18 Soit $\varphi \in Aut(\mathfrak{S}_n)$, si φ transforme les transpositions en transpositions, alors $\varphi \in Int(\mathfrak{S}_n)$.

Preuve : Si φ est un morphisme, il suffit de prouver la propriété pour un système de générateurs de $\mathfrak{S}_n$. On choisit alors le système de générateurs exhibé dans le corollaire 1.27 : $\tau_i = (1\ i+1)$ pour $i \in [\![1, n-1]\!]$. Par hypothèse, $\varphi(\tau_i)$ est aussi une transposition. De plus pour $i \neq j$ $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne sont pas à supports disjoints. En effet si c'était le cas $\varphi(\tau_i)$ et $\varphi(\tau_j)$ commuteraient, or

$$\varphi(\tau_i\tau_j) = \varphi(\tau_i)\varphi(\tau_j) = \varphi(\tau_j)\varphi(\tau_i) = \varphi(\tau_j\tau_j).$$

Donc par bijectivité de φ on aurait que $\tau_i\tau_j = \tau_j\tau_i$ ce qui est faux.
Pour $i = 1$ et $j = 2$ on peut donc noter $\varphi(\tau_1) = (a_1\ a_2)$ et $\varphi(\tau_2) = (a_1\ a_3)$ avec $a_1, a_2, a_3 \in [\![1, n]\!]$ et comme φ est un morphisme bijectif, a_1, a_2, a_3 sont différents. De plus comme τ_3 ne commute ni avec τ_1 ni avec τ_2, le support $\varphi(\tau_3)$ admet une intersection non vide avec le support de $\varphi(\tau_1)$ et celui de $\varphi(\tau_2)$. Supposons que l'on soit dans la cas où $Supp(\varphi(\tau_1)) \cap Supp(\varphi(\tau_2))Supp(\varphi(\tau_3)) = \varnothing$, alors on a obligatoirement $\varphi(\tau_3) = (a_2\ a_3)$ ainsi,

$$\varphi(\tau_1\tau_2\tau_3) = (a_1\ a_2)(a_1\ a_3)(a_2\ a_3) = (a_1\ a_3) = \varphi(\tau_2).$$

Donc par bijectivité de φ on a donc $\tau_1\tau_2\tau_3 = \tau_2$. Ce qui est absurde. On en conclut donc que $a_1 \in Supp(\varphi(\tau_3))$. Ainsi, il existe un élément $a_4 \in [\![1, n]\!]$ différent de a_1, a_2, a_3 tel que $\varphi(\tau_3) = (a_1\ a_4)$. En répétant le argument on se rend compte que pour tout $i \in [\![1, n-1]\!]$ $\varphi(\tau_i) = (a_1\ a_{i+1})$ avec a_{i+1} différent de $a_1, a_2, \dots a_i$.
On a donc obtenu une permutation $\sigma \in \mathfrak{S}_n$ définie par $\sigma(i) = a_i$ telle que pour toutes transpositions de la forme τ_i on ait $\varphi(\tau_i) = \sigma\tau_i\sigma^{-1}$. Comme $(\tau_i)_{i\in[\![1,n]\!]}$ est un système de générateurs de $\mathfrak{S}_n$, on a donc prouvé que $\varphi \in Int(\mathfrak{S}_n)$.

□

La réciproque de ce lemme est évidente grâce au lemme 2.16 et au théorème 1.22. Nous pouvons maintenant passer à la preuve du théorème 2.17.

Preuve : Soit $\varphi \in Aut(\mathfrak{S}_n)$. Comme l'ordre d'une permutation est une propriété algébrique alors l'image de toute transposition par un automorphisme de $\mathfrak{S}_n$ est d'ordre 2. On note

$$T_k = \{(a_1\ a_2)(a_3\ a_4)\dots(a_{2k-1}\ a_{2k}) \text{ tel que } a_i \in [\![1, n]\!] \ a_i \neq a_j \text{ si } i \neq j\}.$$

D'après le théorème 1.22 T_k est une classe de conjugaison de $\mathfrak{S}_n$ d'éléments d'ordre 2. Donc en utilisant le lemme 2.16 pour tous $k \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$ $\varphi(T_k) = T_{k'}$ avec $k' \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$. En particulier, il existe un $k_1 \in [\![1, \lfloor \frac{n}{2} \rfloor]\!]$ tel que $\varphi(T_1) = T_{k_1}$. Montrons que $k = 1$ en raisonnant par l'absurde. Pour cela nous allons calculer le cardinal des T_k par récurrence. Nous allons montrer que

$$\#T_k = \frac{n(n-1)\dots(n-2k+1)}{2^k k!}.$$

Commençons par $T_1 = \{(a_1\ a_2) \text{ tel que } a_i \in [\![1, n]\!] \ a_1 \neq a_2\}$. Nous avons n choix possibles pour a_1 et comme $a_2 \neq a_1$, nous avons $n-1$ choix possibles pour a_2. En procédant ainsi on a compté deux fois chaque transposition ($(a_1\ a_2)$ et $(a_2\ a_1)$), donc $\#T_1 = \frac{n(n-1)}{2}$.
On suppose que la propriété est vraie au rang k, prouvons la au rang $k+1$. Or

$$T_{k+1} = \{\underbrace{(a_1\ a_2)(a_3\ a_4)\dots(a_{2k-1}\ a_{2k})}_{\in T_k}(a_{2k}\ a_{2k+1}) \text{ tel que } a_i \in [\![1, n]\!] \ a_i \neq a_j \text{ si } i \neq j\}$$

Donc $\#T_{k+1} = \#T_k \times \underbrace{(n-2k)(n-2k-1)}_{\text{choix de } a_{2k} \text{ et } a_{2k+1}} \times \underbrace{\frac{1}{2}}_{\text{doublons dernière transpo}} \times \underbrace{\frac{1}{k+1}}_{\text{compte } k+1 \text{ fois même élément}}$

En utilisant l'hypothèse de récurrence on obtient donc que $\#T_{k+1} = \frac{n(n-1)\dots(n-2k-1)}{2^{k+1}(k+1)!}$. Ce qui achève la récurrence.
Or $\varphi(T_1) = T_{k_1}$ et φ est bijectif, donc on a : $\#T_1 = \#T_{k_1}$ et donc

$$2^{k_1-1}(k_1)! = (n-2)\dots(n-2k_1+1).$$

Pour $k_1 = 2$ l'équation devient : $(n-2)(n-3) = 4$, qui n'admet pas de solution sur $\mathbb{N}$ (On a un polynôme de degré 2 qui n'admet pas de racine dans entière).
Pour $k_1 > 3$, l'équation se réécrit : $(n-2)(n-3)\dots(n-k_1+1)\underbrace{\frac{(n-k_1)\dots(n-2k_1+1)}{k_1!}}_{=\binom{n-k_1}{k_1}\in\mathbb{N}} = 2^{k_1-1}$.
Or comme $(n-2)$ ou $(n-3)$ est impair par unicité de la décomposition en facteur premier, on trouve que l'équation considérée n'admet pas de solution.
Pour $k_1 = 3$ l'équation devient : $(n-2)(n-3)(n-4)(n-5) = 2^2 3! = 4!$ ce qui est équivalent à $\binom{n-2}{4} = 1$, on trouve donc $n = 6$.
Donc pour $n \neq 6$ $\varphi(T_1) = T_1$, ainsi en utilisant le lemme 2.18 on conclut que si $n \neq 6$ alors $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$.

□

Corollaire 2.19 Pour $n \neq 6$, $Aut(\mathfrak{S}_n) \simeq \mathfrak{S}_n$

La démonstration précédente ne nous aide pas à comprendre ce qui se passe réellement pour le cas $n = 6$. Nous allons donc un peu nous attarder sur les automorphismes de $\mathfrak{S}_6$. Dans un premier temps montrons le résultat suivant.

Propriété 2.20 Pour $n \neq 4$, les propriétés suivantes sont équivalentes :

1. $Aut(\mathfrak{S}_n) \simeq Int(\mathfrak{S}_n)$
2. Les sous groupes d'indice n de $\mathfrak{S}_n$ sont tous conjugués.

Preuve : Prouvons dans un premier temps que (non 2) $\Rightarrow$ (non 1).
Soit H un sous groupe d'indice n de $\mathfrak{S}_n$. On note $S(i)$ le stabilisateur de $i \in [\![1, n]\!]$ sous l'action naturelle de $\mathfrak{S}_n$ sur $[\![1, n]\!]$, donc $S(i) = \{\sigma \in \mathfrak{S}_n \mid \sigma(i) = i\}$. Alors il est immédiat que $S(i)$ est un sous groupe de $\mathfrak{S}_n$ et que comme il est isomorphe à $\mathfrak{S}_{n-1}$, il est d'indice n. Donc en particulier $S(i)$ n'est pas conjugué à H.
En remarquant que $\mathfrak{S}_n$ agit par translation à gauche sur ${}^{\mathfrak{S}_n}/_H$, on a donc un morphisme

$$\varphi : \mathfrak{S}_n \to \mathfrak{S}({}^{\mathfrak{S}_n}/_H).$$

Montrons que ce morphisme est bijectif, pour cela commençons par remarquer qu'il nous suffit de prouver l'injectivité car $\mathfrak{S}({}^{\mathfrak{S}_n}/_H) \simeq \mathfrak{S}_n$. Or, $Ker(\varphi) = \cap_{\sigma\in\mathfrak{S}_n} \sigma H \sigma^{-1}$, donc $Ker(\varphi) \subset H$, en particulier on a $\#Ker(\varphi) \leqslant \#H = (n-1)! < \frac{n!}{2}$ car $n \geqslant 5$. De plus H est un sous groupe distingué de $\mathfrak{S}_n$, donc le corollaire 2.14 et l'inégalité sur le cardinal de $Ker(\varphi)$ nous assure que $Ker(\varphi) = \{Id\}$. Donc φ est bien bijectif.
Dans cet isomorphisme, le stabilisateur de $H \in {}^{\mathfrak{S}_n}/_H$ est $\varphi(H)$. On considère maintenant f une bijection de ${}^{\mathfrak{S}_n}/_H$ sur $[\![1, n]\!]$ telle que $f(H) = 1$. On en déduit alors un isomorphisme

$$\psi : \sigma({}^{\mathfrak{S}_n}/_H) \to \mathfrak{S}_n.$$

tel que $\psi(\varphi(H)) = S(1)$. Or comme par hypothèse, H et $S(1)$ ne sont pas conjugués, l'automorphisme $\psi \circ \varphi$ n'est pas un automorphisme intérieur.

La réciproque (non 1) $\Rightarrow$ (non 2), se prouve rapidement une fois que l'on sait que l'image d'un sous groupe d'indice n par un automorphisme est encore un sous groupe d'indice n.

□

Remarque 2.21 Dans le cas où $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$, les sous groupes d'indice n de $\mathfrak{S}_n$ sont en fait exactement les $S(i)$. En effet soit H un sous groupe d'indice n de $\mathfrak{S}_n$, alors d'après la propriété 2.20 H est conjugué à tous les $S(i)$. En utilisant le fait que $S(j) = (i\ j)S(j)(i\ j)$ et que les transpositions engendrent $\mathfrak{S}_n$, on prouve qu'il existe un $k \in [\![1, n]\!]$, tel que $H = S(k)$.

Propriété 2.22 On a $Aut(\mathfrak{S}_6) \neq Int(\mathfrak{S}_6)$

Preuve : D'après la propriété 2.20, il suffit de construire un sous groupe d'indice 6 de $\mathfrak{S}_6$, qui n'est pas conjugué aux $S(i)$. Pour ceci, il suffit de trouver un sous groupe H qui opère transitivement sur $[\![1, 6]\!]$.
Soit k le nombre de 5-Sylow de $\mathfrak{S}_5$, d'après le troisième théorème de Sylow, $k|24$ et $k \equiv 1\ (mod\ 5)$. Donc $k = 1$ ou $= 6$. Le cas $k = 1$ est exclu par le corollaire 2.14. Donc $\mathfrak{S}_5$ possède six 5-Sylow. On note X l'ensemble des 5-Sylows de $\mathfrak{S}_5$. Or $\mathfrak{S}_5$ agit sur X par conjugaison, transitivement et fidèlement (2.14). On a donc un morphisme de groupe injectif :

$$\varphi : \mathfrak{S}_5 \to \mathfrak{S}(X) \simeq \mathfrak{S}_6$$

De plus comme $\mathfrak{S}_5$ agit transitivement sur X, alors le sous groupe $\varphi(\mathfrak{S}_5)$ convient.

□

3 Applications

3.1 Les polynômes symétriques

Nous allons maintenant étudier les polynômes symétriques à coefficients dans un anneau commutatif A. Soit $P \in A[X_1, \ldots, X_n]$ on notera :

$$P = \sum_{0 \leqslant m_1, \ldots, m_n} a_{m_1,\ldots,m_n} X_1^{m_1} \cdots X_n^{m_n}$$

où les coefficients $a_{m_1,\ldots,m_n}$ sont presque tous nuls.

Dans la suite nous étudierons les points fixes de $A[X_1, \ldots, X_n]$ sous l'action suivante :

$$\begin{array}{rcl} \mathfrak{S}_n \times A[X_1 \ldots X_n] & \longrightarrow & A[X_1, \ldots, X_n] \\ (\sigma, P) & \longmapsto & P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \end{array}$$

Définition - Propriété 3.1 Soit $P \in A[X_1, \ldots, X_n]$. On dit que P est symétrique s'il est fixe sous l'action de $\mathfrak{S}_n$ décrite précédemment, ie si pour toute permutation σ de $\mathfrak{S}_n$

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n).$$

L'ensemble des polynômes symétriques est une sous A algèbre de $A[X_1, \ldots, X_n]$.

Exemple 3.2 Le polynôme $P = X_1 + X_2 + X_3$ est un polynôme symétrique pour $n = 3$ mais ne l'est pas pour $n = 4$.

Définition - Propriété 3.3 Soit $j \in [\![1, n]\!]$, le polynôme

$$\Sigma_{j,n} := \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} X_{i_1} \dots X_{i_j}$$

est un polynôme symétrique que l'on appellera le *j-ème polynôme symétrique élémentaire* de $A[X_1, \dots, X_n]$.

Théorème 3.4 (Structure des polynômes symétriques)
Pour tout polynôme symétrique $P \in A[X_1, \dots, X_n]$, il existe un unique polynôme $Q \in A[T_1, \dots, T_n]$ tel que

$$P = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n}).$$

Preuve : L'existence d'un tel polynôme se prouve à l'aide d'une double récurrence sur le degré $d \geqslant 0$ de P et sur le nombre de variables $n \geqslant 1$ de l'anneau des polynômes dans lequel on travaille. Pour $n = 1$, on a $\Sigma_{1,1} = X_1$ ainsi en prenant $Q = P$, on obtient que $P(X_1) = Q(\Sigma_{1,1})$. On suppose maintenant que la propriété est vraie pour $n - 1 \geqslant 1$. Si le polynôme est constant, alors en prenant $Q = P$ on a clairement $P(X_1, \dots, X_n) = Q(X_1, \dots, X_n)$. On suppose maintenant que le résultat est vrai pour des polynômes à n variables et de degré $d - 1$. Soit $P \in A[X_1, \dots, X_n]$ de degré d, alors $P(X_1, \dots, X_{n-1}, 0)$ étant un polynôme symétrique de $A[X_1, \dots, X_{n-1}]$ par hypothèse de récurrence, il existe $Q_1 \in A[X_1, \dots, X_{n-1}]$ tel que

$$\begin{aligned} P(X_1, \dots, X_{n-1}, 0) &= Q_1(\Sigma_{1,n-1}, \dots, \Sigma_{n-1,n-1}) \\ &= Q_1(\Sigma_{1,n}(X_1, \dots, X_{n-1}, 0), \dots, \Sigma_{n-1,n}(X_1, \dots, X_{n-1}, 0)). \end{aligned}$$

Ainsi, le polynôme $P_1 = P - Q_1$ est symétrique de degré inférieur ou égal à d dans $A[X_1, \dots, X_n]$. De plus $P_1(X_1, \dots, X_{n-1}, 0) = 0$ donc $P_1 = \sum a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ avec les $a_{i_1,\dots,i_n}$ et les i_n non nuls. Or en notant $\tau_k := (k, n)$,

$$\begin{aligned} P_1(X_{\tau_k(1)}, \dots, X_{\tau_k(n)}) &= P_1(X_1, \dots, X_{k-1}, X_n, X_{k+1}, \dots, X_k) \\ &= P_1(X_1, \dots, X_n) \end{aligned}$$

et en prenant $X_n = 0$, on obtient que $P_1(X_1, \dots, X_{k-1}, 0, X_{k+1}, \dots, X_k) = 0$, ce qui nous permet d'affirmer que pour tout $k \in [\![1, n_1]\!]$ les exposant i_k sont non nuls. Donc,

$$P_1 = \left(\sum a_{i_1,\dots,i_n} X_1^{i_1 - 1} \cdots X_n^{i_n - 1} \right) X_1 \dots X_n = P_2 \Sigma_{n,n}.$$

De plus en utilisant l'égalité ci-dessus on peut obtenir que P_2 est également un polynôme symétrique. Le polynôme P_2 est donc symétrique et de degré au plus $d-1$. On peut donc lui appliquer la deuxième hypothèse de récurrence : il existe $Q_2 \in A[X_1, \dots, X_n]$ tel que $P_2 = Q_2(\Sigma_{1,n}, \dots, \Sigma_{n,n})$.
Finalement,

$$\begin{aligned} P(X_1, \dots, X_n) &= P_1(X_1, \dots, X_n) + Q_1(\Sigma_{1,n}, \dots, \Sigma_{n-1,n}) \\ &= Q_2(\Sigma_{1,n}, \dots, \Sigma_{n,n}) \Sigma_{n,n} + Q_1(\Sigma_{1,n}, \dots, \Sigma_{n-1,n}) \\ &= Q(\Sigma_{1,n}, \dots, \Sigma_{n,n}) \end{aligned}$$

où $Q \in A[X_1, \ldots, X_n]$.
L'existence étant maintenant établie, il nous reste à prouver l'unicité d'un tel polynôme, ce qui revient à prouver que l'égalité $Q(\Sigma_{1,n}, \ldots, \Sigma_{n,n}) = 0$ implique que $Q = 0$. Pour cela raisonnons une nouvelle fois par double récurrence. Si Q est un polynôme à une seule variable, comme $X_1 = \Sigma_{1,1}$, on obtient directement le résultat. On suppose maintenant que l'hypothèse est vraie pour tout polynôme à $n-1$ variables. Si Q est un polynôme constant alors l'hypothèse est évidement vérifiée. On admet alors que l'hypothèse est vérifiée pour tous polynômes à n variables et de degré inférieur ou égal à $d-1$. Soit $Q \in A[X_1, \ldots, X_n]$ de degré d tel que $Q(\Sigma_{1,n}, \ldots, \Sigma_{n,n}) = 0$. Réalisons la division euclidienne de Q dans $A[X_1, \ldots, X_{n-1}][X_n]$ par X_n :

$$Q(X_1, \ldots, X_n) = S(X_1, \ldots, X_n)X_n + R(X_1, \ldots, X_{n-1}).$$

La condition $Q(\Sigma_{1,n}, \ldots, \Sigma_{n,n}) = 0$ et l'évaluation en $X_n = 0$ nous permet d'affirmer que $R(\Sigma_{1,n-1}, \ldots, \Sigma_{n-1,n-1}) = 0$ et par hypothèse de récurrence sur n on trouve que $R = 0$. On a donc

$$0 = Q(\Sigma_{1,n}, \ldots, \Sigma_{n,n}) = S(\Sigma_{1,n}, \ldots, \Sigma_{n,n})\Sigma_{n,n}$$

Donc, $S(\Sigma_{1,n}, \ldots, \Sigma_{n,n}) = 0$ avec S qui est de degré au plus égal à $d-1$, ainsi en utilisant l'hypothèse de récurrence sur le degré on trouve que $S = 0$. Donc $Q = 0$. Ce qui établit l'unicité du théorème.

□

Propriété 3.5 (Relations coefficients racines)
Soit A un anneau, soient $P \in A[X]$ et $(\alpha_1, \ldots, \alpha_n) \in A^n$. Les conditions suivantes sont équivalentes :

1. $P(X) = (X - \alpha_1) \ldots (X - \alpha_n)$
2. $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ où $\forall i \in [\![1, n]\!], a_{n-i} = (-1)^i \Sigma_{i,n}(\alpha_1, \ldots, \alpha_n)$

Preuve : Il suffit de développer l'expression de P donnée dans 1.

□

Application 3.6 (Théorème de Kronecker)
Soit P un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose $P(0) \neq 0$. Alors toutes les racines de P sont des racines de l'unité.

Preuve : Notons $\Omega_n = \{P \in \mathbb{Z}[X] \text{ tel que } \mathcal{Z}(P) \subset \mathcal{D}(0,1) \text{ et de degré } n\}$. Montrons dans un premier temps que Ω_n est de cardinal fini.
Soit $P = \sum_{i=1}^{n} a_i X^i$ et $z_1, \ldots, z_n$ les racines de P. En utilisant les relations coefficients racines de la propriété 3.5 on peut écrire :

$$|a_{n-i}| = |\Sigma_{i,n}(z_1, \ldots, z_n)| \leqslant \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} 1 = \binom{n}{i}.$$

De plus comme pour tout i, $a_i \in \mathbb{Z}$, cela nous montre qu'il existe un nombre fini de polynômes dans Ω_n.
On note maintenant $P_k = (X - z_1^k) \ldots (X - z_n^k) = \sum_{i=0}^{n} c_{j,k} X^{n-i}$. Montrons que pour tout k entier naturel non nul, $P_k \in \Omega_n$.
Par construction des $c_{j,k}$, ce sont des polynômes symétriques à coefficients entiers en les z_i. Ainsi d'après le théorème de structure des polynômes symétriques (3.4), il existe $R_{j,k}$, un polynôme à coefficients entiers, tel que

$$c_{j,k} = R_{j,k}(\Sigma_{1,n}(z_1, \ldots, z_n), \ldots, \Sigma_{n,n}(z_1, \ldots, z_n)).$$

Par conséquent, comme les $\Sigma_{j,n}(z_1, \ldots, z_n)$ sont les coefficients de P, ils appartiennent à $\mathbb{Z}$, donc $c_{j,k} \in \mathbb{Z}$. Ainsi on a bien $P_k \in \Omega_n$.
Le cardinal de Ω_n étant fini, l'ensemble des racines des polynômes de Ω_n est donc lui aussi de cardinal fini. Ainsi, pour $i \in [\![1, n]\!]$, si on considère l'application $k \longmapsto z_i^k$, qui va de $\mathbb{N}$ (de cardinal infini) dans l'ensemble des racines des polynômes de Ω_n (de cardinal fini), elle ne peut pas être injective. Donc il existe $k, k' \in \mathbb{N}$ différents l'un de l'autre, tel que $z_i^k = z_i^{k'}$, ce qui s'écrit aussi $z_i^{k-k'} = 1$ avec $k - k' \neq 0$. Donc pour tout i, z_i est une racine de l'unité.

□

Remarque 3.7 En notant a_n le cardinal de Ω_n, on peut prouver l'égalité suivante :

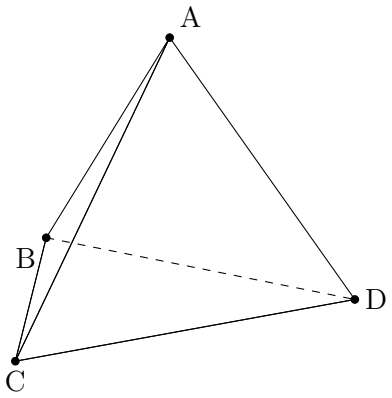
$$\forall z \in \mathbb{C} \text{ tel que } |z| < 1, \quad \sum_{n=1}^{\infty} a_n z^n = \prod_{n=0}^{\infty} \frac{1}{1 - z^{\varphi(n)}} \quad \text{où } \varphi \text{ l'indicatrice d'Euler.}$$

3.2 Les isométries du tétraèdre et $\mathfrak{S}_4$

Définition 3.8 Le groupe $Is(X)$ des isométries d'un objet $X \subset \mathbb{R}^3$ est le sous groupe des isométries de l'espace affine euclidien $\mathbb{R}^3$ qui stabilise X.

Théorème 3.9 Le groupe des isométries du tétraèdre Δ_4 est $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$.

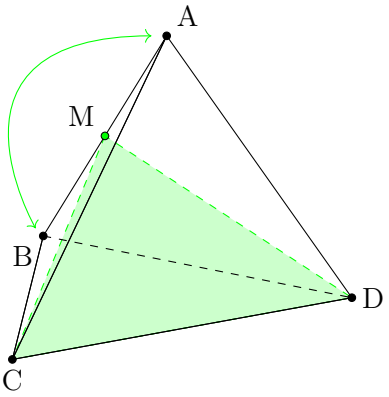
Preuve : Notons A, B, C, D les sommets du tétraèdre, comme dans la figure ci-dessous.



Les sommets du tétraèdre sont ses points extrémaux, donc le groupe $\mathrm{Is}(\Delta_4)$ agit par permutation sur l'ensemble $\{A, B, C, D\}$. Puisque (A, B, C, D) constitue une base affine de l'espace, on dispose donc d'une injection

$$\varphi : \mathrm{Is}(\Delta_4) \hookrightarrow \mathfrak{S}_{\{A,B,C,D\}} \simeq \mathfrak{S}_4.$$

Considérons M le milieu du segment $[AB]$ et soit r la réflexion par rapport au plan (MCD). Alors r réalise la transposition $(A\ B)$ dans $\mathfrak{S}_{\{A,B,C,D\}}$ et $r \in \mathrm{Is}(\Delta_4)$.



Par symétrie des rôles de A, B, C et D, toutes les transpositions sont dans l'image de φ et par conséquent, φ est surjective et est donc un isomorphisme.

□

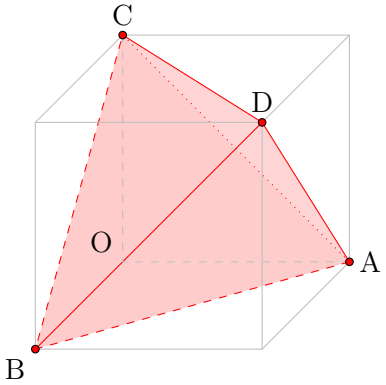
Théorème 3.10 La table des caractères de $\mathfrak{S}_4$ est donnée par :

	Id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
$triv$	1	1	1	1	1
ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_{Δ_4}	3	1	0	-1	-1
$\chi_{\Delta_4} \cdot \varepsilon$	3	-1	0	1	-1

Preuve : **Étape 1 :** (caractères de degré 1)
Les caractères de degré 1 de $\mathfrak{S}_4$ sont les morphismes de $\mathfrak{S}_4$ dans $\mathbb{C}^*$, grâce au théorème 2.4 on sait qu'il n'existe que le morphisme trivial $triv$ et la signature ε. On obtient donc le début de table

	Id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
$triv$	1	1	1	1	1
ε	1	-1	1	-1	1

Étape 2 : (une représentation par action sur le tétraèdre)
Fixons le tétraèdre inscrit dans le cube, en rouge dans la figure ci-dessous, de sorte que si O désigne l'origine de $\mathbb{R}^3$, les vecteurs $\overrightarrow{OA}, \overrightarrow{OB}$ et $\overrightarrow{OC}$ forment la base canonique de $\mathbb{R}^3$ en tant qu'espace vectoriel et que $\overrightarrow{OD}$ a pour coordonnées $(1, 1, 1)$.



Considérons la représentation $(\mathbb{R}^3, \rho)$ induite par l'isomorphisme $\mathfrak{S}_4 \simeq \mathrm{Is}(\Delta_4)$, dont on note χ_{Δ_4} le caractère.
Notons O' le barycentre des points A, B, C, D, de sorte que (O', A, B, C) forme une base affine de $\mathbb{R}^3$. Ainsi, si $\mathcal{B}$ est la base $(\overrightarrow{O'A}, \overrightarrow{O'B}, \overrightarrow{O'D})$, en utilisant la relation $\overrightarrow{O'A} + \overrightarrow{O'B} + \overrightarrow{O'C} + \overrightarrow{O'D} = \overrightarrow{0}$, les matrices des $\rho(g)$ s'écrivent :

$$\mathscr{M}_{\mathcal{B}}(A\ B) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathscr{M}_{\mathcal{B}}(A\ B\ C) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathscr{M}_{\mathcal{B}}(A\ B\ C\ D) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix},$$

$$\mathscr{M}_{\mathcal{B}}(A\ B)(C\ D) = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}.$$

On en déduit donc le caractère χ_{Δ_4}, qui est bien irréductible puisque

$$\langle \chi_{\Delta_4}, \chi_{\Delta_4} \rangle = \frac{1}{24}(1 \times 3^2 + 6 \times 1^2 + 8 \times 0^2 + 6 \times (-1)^2 + 3 \times (-1)^2) = 1,$$

ce qui nous permet de continuer à remplir la table

	Id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
$triv$	1	1	1	1	1
ε	1	-1	1	-1	1
χ_{Δ_4}	3	1	0	-1	-1

Étape 3 : (multiplier par ε)
On remarque que si l'on considère le produit tensoriel entre la représentation standard et ε, on obtient une représentation dont le caractère est $\chi_{\Delta_4} \cdot \varepsilon$. Or,

$$\langle \chi_{\Delta_4} \cdot \varepsilon, \chi_{\Delta_4} \cdot \varepsilon \rangle = \frac{1}{\#\mathfrak{S}_4} \sum_{\sigma \in \mathfrak{S}_4} \chi_{\Delta_4}(\sigma) \cdot \varepsilon(\sigma) \overline{\chi_{\Delta_4}(\sigma) \cdot \varepsilon(\sigma)} = \frac{1}{\#\mathfrak{S}_4} \sum_{\sigma \in \mathfrak{S}_4} \chi_{\Delta_4}(\sigma) \overline{\chi_{\Delta_4}(\sigma)} = \langle \chi_{\Delta_4}, \chi_{\Delta_4} \rangle = 1,$$

donc $\chi_{\Delta_4} \cdot \varepsilon$ est un caractère irréductible, ce qui nous permet à nouveau de compléter notre table

	Id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
$triv$	1	1	1	1	1
ε	1	-1	1	-1	1
χ_{Δ_4}	3	1	0	-1	-1
$\chi_{\Delta_4} \cdot \varepsilon$	3	-1	0	1	-1

Enfin, on sait qu'il nous reste un dernier caractère à déterminer. Puisque la somme des carrés des dimension des caractères irréductibles est égale à l'ordre de $\mathfrak{S}_4$ (*i.e.* 24), le degré de ce dernier caractère est 2 et nous le nommerons donc χ_2. Comme précédemment, $\chi_2 \cdot \varepsilon$ est encore un caractère irréductible, nécessairement identique à χ_2 puisqu'il est lui aussi de degré égal à 2. Ainsi, on a $\chi_2(1\ 2) = \chi(1\ 2\ 3\ 4) = 0$, puisque la signature de ces éléments vaut -1. Notons pour le moment $a = \chi(1\ 2\ 3)$ et $b = \chi((1\ 2)(3\ 4))$. Les relations d'orthogonalité nous donnent

$$\langle \chi_2, \chi_{\Delta_4} \rangle = 0 = \frac{1}{24}(1 \cdot 2 \cdot 3 + 6 \cdot 0 \cdot 1 + 8 \cdot a \cdot 0 + 6 \cdot 0 \cdot (-1) + 3 \cdot b \cdot (-1)) = \frac{1}{24}(6 - 3b),$$

d'où l'on déduit que $b = 2$ et

$$\langle \chi_2, triv \rangle = 0 = \frac{1}{24}(1 \cdot 2 \cdot 1 + 6 \cdot 0 \cdot 1 + 8 \cdot a \cdot 1 + 6 \cdot 0 \cdot 1 + 3 \cdot 2 \cdot 1) = \frac{1}{24}(2 + 8a + 6),$$

qui nous permet de conclure que $a = -1$. Finalement, on a bien la table annoncée.

□